



РЕШЕНИЯ CISCO SYSTEMS ДЛЯ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ СТАНДАРТА СТО БР ИББС-1.0-2006 БАНКА РОССИИ

ВВЕДЕНИЕ

По данным опроса Межбанковского Финансового Дома (МФД) и Ассоциации Российских Банков (АРБ) проведенного в 2003 году, бизнес-процессы 88% российских финансовых организаций полностью опираются на информационные технологии. Такая зависимость не позволяет эффективно реализовывать бизнес-процессы без решения вопросов безопасности информационной инфраструктуры.

Банк по праву считается организацией повышенного риска, болезненно реагирующей на любые удары по имиджу. Эпидемии червей, нарушение функционирования серверов платежной информации, перехват важной финансовой информации, утечка клиентской базы и другие угрозы наносят очень серьезный ущерб по репутации и являются серьезным препятствием для развития бизнеса любого банка. А как показывает статистика, в число компьютерных атак на финансовые учреждения увеличивается год от года. Как только становится известным какое-либо неблагоприятное событие (в т.ч. и связанное с нарушением защищенности автоматизированной банковской системы), то у банка сразу же могут наступить серьезные трудности с рефинансированием, начнется отказ клиентов от возобновления вкладов и их уход к конкурентам, что в свою очередь может привести к кризису ликвидности.

Помимо репутации, важным является сохранение в тайне различной внутренней информации, на которой зачастую и строится принятие решений, измеряемых десятками и сотнями миллионов долларов. Утечка такой конфиденциальной информации позволяет игрокам банковского рынка делать упреждающие ходы, препятствующие тем или иным финансовым мероприятиям (слияния, покупка, продажа и т.д.), что также сказывается на бизнесе любого банка.

Также надо учитывать, что банк, работая с большим числом физических и юридических лиц, должен быть, с одной стороны, открытым, прозрачным и доступным для всех своих вкладчиков, а с другой – защищенным и минимизирующим ущерб от различных умышленных и неумышленных действий собственных сотрудников, клиентов, а также посторонних лиц.

Как субъекты экономики банки относятся к критичным национальным инфраструктурам и находятся в зоне повышенного внимания со стороны государства. Ведь кризис и дестабилизация работы одного из банков, может привести к нарушению функционирования всей банковской системы и даже ее обвалу, что в свою очередь создает угрозу государству. Учитывая степень зависимости банков от используемых информационных технологий, угрозы информационной безопасности представляют собой реальную опасность для всей банковской системы. Неслучайно, в 2004 году Указом Президента России от 16 августа № 1085 на преемницу Государственной технической комиссии – Федеральную службу по техническому и экспортному контролю возложена задача обеспечения безопасности в ключевых системах информационной инфраструктуры, оказывающих существенное влияние на безопасность государства. К таким ключевым системам в России скорее всего будут отнесены и организации банковской системы.

СТАНДАРТ БАНКА РОССИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Понимая данную проблему и являясь ответственным за банковскую систему страны, Центральный банк с 1 декабря 2004 года (Распоряжением Банка России от 18 ноября 2004 года № Р-609) ввел в действие стандарт «Обеспечение информационной безопасности организаций банковской системы Российской Федерации», нацеленный на повышение уровня защищенности российских банков и защиту банковской тайны вкладчиков.

В настоящее время действует уже вторая редакция данного Стандарта СТО БР ИББС-1.0-2006 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (далее Стандарт), доработанная в учетом опыта практического применения первой редакции Стандарта, принятая и введенная в действие Распоряжением Банка России № Р-27 от 26.01.2006.

Стандарт распространяется на организации банковской системы Российской Федерации (далее БС РФ), к которым относятся Банк России, кредитные организации, филиалы и представительства иностранных банков, и устанавливает положения (политики, требования и т.п.) по обеспечению информационной безопасности. Стандарт рекомендован для применения путем включения ссылок на него, а также прямого использования устанавливаемых в нем положений во внутренних нормативных и методических документах организаций БС РФ, а также в заключаемых банками договорах.

Положения Стандарта применяются на добровольной основе, если только в отношении конкретных положений обязательность не установлена нормативными документами или условиями договора, но могут быть введены в качестве обязательных в случае, если возникнет такая необходимость. Учитывая общемировую тенденцию по усилению контроля над кредитно-финансовой сферой экономики со стороны государственных и отраслевых регуляторов, можно предположить, что данный Стандарт из разряда «рекомендательный» вскоре будет рассматриваться как «обязательный для исполнения».

Основными целями Стандарта являются:

- повышение доверия к БС РФ;
- повышение стабильности функционирования финансовых организаций и на этой основе – стабильности функционирования БС РФ в целом;
- достижение адекватности мер по защите от реальных угроз информационной безопасности;
- предотвращение и/или снижение ущерба от инцидентов информационной безопасности.

Данные цели достигаются путем решения задач:

- установление единых требований по обеспечению информационной безопасности БС РФ;
- повышение эффективности мероприятий по обеспечению и поддержанию информационной безопасности организаций БС РФ.

Компания Cisco Systems, являясь лидером не только мирового, но и российского рынка средств обеспечения информационной безопасности, предлагает организациям БС РФ широкий спектр защитных решений, учитывающих практически все требования нового Стандарта.

ТРЕБОВАНИЯ СТАНДАРТА И МЕТОДЫ ИХ РЕАЛИЗАЦИИ

В разделе 6 Стандарта перечислены основные принципы обеспечения защиты информации в российских банках. Среди них – своевременность обнаружения проблем, прогнозируемость развития проблем и оценка их влияния на бизнес-цели, а также контролируемость защитных мер.

Рассмотрим, как решения компании Cisco Systems позволяют эффективно реализовать данные принципы, а также ряд других требований, указанных в разделе 8 Стандарта.

Защищенная архитектура

Для защиты от угроз (перечисленных в п.8.2.3.5 Стандарта):

- внесения разработчиком автоматизированной банковской системы (АБС) дефектов на уровне архитектурных решений,
- неадекватной (неполной, противоречивой, некорректной и т.п.) реализации требований к АБС
- неверного конфигурирования АБС

компания Cisco Systems предлагает специальную архитектуру безопасности корпоративных сетей SAFE, основная цель которой состоит в том, чтобы предоставить финансовым организациям информацию о современном опыте проектирования и развертывания защищенных сетей. Архитектура SAFE призвана помочь тем, кто проектирует сети и анализирует требования к сетевой безопасности. SAFE исходит из принципа глубоко эшелонированной обороны банковских автоматизированных систем от внешних и внутренних атак. Этот подход нацелен не на механическую установку межсетевых экранов и системы обнаружения атак, а на анализ ожидаемых угроз и разработку методов борьбы с ними. Эта стратегия приводит к созданию многоуровневой системы защиты, при которой прорыв одного уровня не означает прорыва всей системы безопасности.

Архитектура Cisco SAFE с максимальной точностью моделирует функциональные потребности корпоративных сетей современных финансовых организаций и решает следующие задачи (в порядке приоритетности):

- Безопасность и борьба с атаками на основе политик.
- Внедрение мер безопасности по всей инфраструктуре (а не только на специализированных устройствах защиты).
- Безопасное управление и отчетность.
- Идентификация, аутентификация, авторизация и контроль доступа пользователей и администраторов для доступа к критически важным сетевым ресурсам.
- Обнаружение атак на критически важные ресурсы и подсети.
- Поддержка новых сетевых приложений.

К ключевым достоинствам SAFE можно отнести:

- Обеспечение основы для построения безопасных, доступных и интегрированных сетей.
- Открытую модульную структуру.
- Упрощение разработки, внедрения и управления сетевой безопасностью.
- Обеспечение масштабируемости решений.
- Эффективное поэтапное внедрение.

Применение сертифицированных средств защиты информации

Компания Cisco Systems приняла на себя обязательства по сертификации своих решений по информационной безопасности в соответствии с требованиями, принятыми в разных странах. В России компания Cisco Systems сертифицировала свои:

- межсетевые экраны Cisco Pix и Catalyst FWSM,
- маршрутизаторы с ОС Cisco IOS,
- коммутаторы Cisco Catalyst,
- сетевые и хостовые системы обнаружения атак Cisco IDS 42xx, Catalyst IDSM-2 и Cisco Security Agent,
- а также систему управления CiscoWorks VPN/Security Management Solution

на соответствие соответствующим руководящим документам и техническим условиям, принятым Федеральной службой по техническому и экспортному контролю (ФСТЭК).

Общее число выданных ФСТЭК (бывшая Государственная техническая комиссия при Президенте России) компании Cisco Systems сертификатов давно превысило 240, что существенно превышает число сертификатов, полученных какой-либо другой компанией (российской или зарубежной), работающей на рынке информационной безопасности. Таким образом, решения компании Cisco Systems удовлетворяют требованию, указанному в п.8.2.4.2 и п.8.2.8.7 Стандарта.

Идентификация, аутентификация и авторизация

Cisco Secure Access Control Server (ACS) – программное или программно-аппаратное решение, предназначенное для централизованной идентификации, аутентификации, авторизации и управления доступом, прописанных в п.8.2.4.3 Стандарта. При этом данные защитные механизмы реализуются через все устройства и решения компании Cisco Systems. При помощи ACS можно управлять доступом на маршрутизаторах и коммутаторах, средствах построения VPN и межсетевых экранах, узлах IP-телефонии и беспроводных точках и клиентах, устройствах хранения и контроля контента, а также на различных типах удаленного доступа (широкополосный, DSL, dialup) и т.д.

Таблица 1. Основные возможности Cisco Secure Access Control Server

Основные возможности	
<ul style="list-style-type: none"> • Поддержка аутентификации LDAP и ODBC, Active Directory и NDS, RADIUS и TACACS+, CHAP и MS-CHAP, PAP и ARA, и т.д. • Поддержка стандарта 802.1x (режимы EAP-TLS, PEAP, Cisco LEAP, EAP-FAST и EAP-MD5) • Авторизация команд на устройствах • Ограничение доступа по времени, числу сессий и другим контролируемым параметрам • Создание профилей пользователей и групп • Интеграция с решениями для однократных паролей и токенов 	<ul style="list-style-type: none"> • Возможность проверки дополнительных условий перед разрешением доступа в сеть • Интеграция с технологией контроля доступа в сеть Network Admission Control • Интеграция с PKI и поддержка списка отозванных сертификатов (CRL) • Регистрация всех попыток доступа пользователей • Генерация отчетов • Возможность поставки в виде специального устройства с защищенной ОС

Локализация узла, зараженного вирусом

Согласно п.8.2.5.5 Стандарта при обнаружении антивирусом зараженного вредоносной программой компьютера, он должен быть локализован с целью предотвращения дальнейшего развития эпидемии. Для решения этой важной задачи компания Cisco Systems разработала новую технологию контроля доступа в сеть – Network Admission Control (NAC), позволяющую предотвратить доступ к корпоративным ресурсам или сети оператора связи устройств, не соответствующих политике безопасности (заражен вредоносной программой, отсутствует или устарел антивирус, отсутствуют патчи и Service Pack'и, отсутствуют средства защиты и иное программное обеспечение). В случае обнаружения такого несоответствия доступ узла либо блокируется, либо перенаправляется в карантинную сеть, в которой на узел может быть установлено отсутствующее программное обеспечение.

Контроль соответствия политике безопасности реализуется как можно ближе к возможному источнику нарушения – на маршрутизаторе Cisco или VPN 3000 Concentrator, коммутаторе Catalyst или точке беспроводного доступа, межсетевом экране Cisco Pix или многофункциональном защитном устройстве Cisco ASA, в которые встроена поддержка NAC, не требующая дополнительного лицензирования.

О своей поддержке и участии в NAC уже объявили такие компании, как Trend Micro, McAfee, Symantec и IBM (Tivoli), а также Computer Associates, Altiris, Internet Security Systems (ISS), Sophos, Panda, Check Point, Лаборатория Касперского и многие другие.

Таблица 2. Основные возможности Cisco Network Admission Control

Основные возможности	
<ul style="list-style-type: none"> • Поддержка любых типов доступа (проводной, беспроводной, коммутируемый, широкополосный и т. д.) • Обеспечение соответствия политике безопасности независимо от желания пользователя • Поддержка EAP over UDP и EAP over 802.1x • Прозрачность для пользователя • Поддержка ОС Windows, Linux и Solaris • Помещение несоответствующего узла в карантин путем применения списков контроля доступа ACL или URL Redirection, а также VLAN и PACL 	<ul style="list-style-type: none"> • Решение парадокса “пользователь имеет право доступа в сеть, а его компьютер – нет” • Мультивендерное решение: интеграция с Altiris, BigFix, IBM, McAfee, Qualys, Symantec, Trend Micro (всего более 70 компаний) • Поддержка широкого спектра оборудования: маршрутизаторы, коммутаторы, VPN-концентраторы, точки беспроводного доступа • Интеграция с системами Cisco MARS, Cisco SIMS • Полная совместимость с системой Microsoft NAP (Network Access Protection)

В том случае, если защищаемая сеть построена не на оборудовании Cisco, то внедрить технологию NAC можно с помощью Cisco NAC Appliance.

Таблица 3. Основные возможности Cisco NAC Appliance

Основные возможности	
<ul style="list-style-type: none"> • Независимость от производителя сетевого оборудования (в режиме in-band) • Интеграция с Kerberos, LDAP, RADIUS, Active Directory, S/Ident и другими методами аутентификации • Сканирование защищенности ОС Windows, MacOS, Linux, Xbox, PlayStation 2 и КПК с помощью Cisco Clean Access Agent • Поддержка антивирусов CA, F-Secure, Eset, Лаборатории Касперского, McAfee, Panda, Drweb, Sophos, Symantec, TrendMicro и других средств защиты компьютера 	<ul style="list-style-type: none"> • Помещение несоответствующего узла в карантин путем применения списков контроля доступа ACL или VLAN • Создание “белого” списка узлов для ускорения их доступа к ресурсам сети • Автоматическая установка отсутствующих обновлений, устаревших антивирусных баз или новых версий средств защиты • Прозрачный аудит • Поддержка русского языка • Централизованное web-управление

Защита дистанционного обслуживания клиентов и при использовании ресурсов Интернет

Согласно п.8.2.6.2 Стандарта для защиты автоматизированной банковской системы при дистанционном обслуживании клиентов через Интернет должны использоваться межсетевые экраны (МСЭ). Компания Cisco Systems предлагает различные типы МСЭ, ориентированных как на защиту периметра, так и для защиты внутренней сети банка – Cisco Pix, Cisco ASA 5500, Cisco FWSM, Cisco IOS Firewall.

Многофункциональный программно-аппаратный комплекс Cisco ASA 5500 предназначен для решения сразу нескольких задач – разграничения доступа к сетевым ресурсам, защиты от атак, защиты взаимодействия с удаленными территориями, блокирования вирусов, червей, шпионского ПО и других вредоносных программ, спама и атак типа “фишинг”. Это достигается за счет объединения в одном устройстве лучших в своем классе защитных средств – межсетевого экрана Cisco Pix, системы предотвращения атак Cisco IPS и Cisco VPN 3000 Concentrator.

Модульная архитектура Cisco Adaptive Identification and Mitigation (AIM) позволяет наращивать защитные возможности Cisco ASA 5500 новыми функциями (по мере разработки новых интегрируемых модулей) – контроль электронной почты и web-трафика

(фильтрация URL), антивирусная защита, антиспам, антифишинг, Network Admission Control и т. п. Этот комплекс незаменим для банковских отделений или удаленных филиалов банков, не имеющих возможности внедрить несколько отдельных защитных устройств. Широкий спектр моделей Cisco ASA 5500, ориентированных на защиту финансовых организаций разного масштаба, обеспечивает их безопасность, производительность и надежность.

Таблица 4. Основные возможности Cisco ASA 5500

Основные возможности	
<ul style="list-style-type: none"> • Управление с помощью Cisco Adaptive Security Device Manager • Поддержка VLAN • Поддержка отказоустойчивых конфигураций (Active/Standby и Active/Active) • Встроенная система корреляции событий Risk Rating, Meta Event Generator • Поддержка OSPF, PIM, IPv6, QoS • Поддержка виртуальных и прозрачных МСЭ • Контроль протоколов и приложений (web, e-mail, FTP, голос и мультимедиа, СУБД, операционные системы, GTP/GPRS, ICQ, P2P и т. П.) 	<ul style="list-style-type: none"> • Контроль всего спектра протоколов для IP-телефонии и мультимедиа – H.323, SIP, SCCP, MGCP, RTSP и т.д. • Защита от атак “переполнение буфера”, нарушения RFC, аномалий, подмены адреса • Организация SSL и IPSec VPN • Отражение вирусов, червей и вредоносных программ • в протоколах http, FTP, SMTP и POP3 • Механизм Syslog to ACL Correlation • Контроль до 8 сетевых интерфейсов • Скрытие топологии защищаемой сети с помощью трансляции адресов (NAT) и портов (PAT)

Таблица 5. Модельный ряд Cisco ASA 5500

	5505 Base/Security Plus	5510 Base/Security Plus	5520	5540	5550
Производительность МСЭ, Мбит/сек	150	300	450	650	1200
Производительность МСЭ и отражения атак (МСЭ + модуль IPS), Мбит/сек	Недоступно в текущий момент	До 150 с AIP-SSM-10 До 300 с AIP-SSM-20	До 225 с AIP-SSM-10 До 375 с AIP-SSM-20	До 450 с AIP-SSM-20	Недоступно
Производительность VPN, Мбит/сек	100	170	225	325	425
Количество одновременно поддерживаемых сессий	10000 / 25000*	50000 / 130000*	280000	400000	650000
Число IPSec VPN-туннелей	10 / 25**	250	750	5000	5000
Число SSL VPN-туннелей**	25	250	750	2500	5000
“Виртуальные” МСЭ (включено/максимум)	0 / 0	0 / 0 (Base) 2 / 5 (Security)	2 / 20	2 / 50	2 / 50

	5505 Base/Security Plus	5510 Base/Security Plus	5520	5540	5550
Кластеризация и балансировка VPN	Нет	Нет	Да	Да	Да
Поддерживаемые физические интерфейсы	8 Fast Ethernet, 2 с поддержкой питания по Ethernet (PoE)	3 Fast Ethernet и 1 порт управления / 5 + Fast Ethernet***	4 Gigabit Ethernet + 1 Fast Ethernet	4 Gigabit Ethernet + 1 Fast Ethernet	8 Gigabit Ethernet + 1 Fast Ethernet
Поддержка дополнительного четырехпортового модуля Gigabit Ethernet	Нет	Да	Да	Да	Нет
Поддерживаемые логические интерфейсы VLAN 802.1q	3 (без транкинга); 3	10 / 25*	100	200	200
Разъем для Flash / порт(ы) USB 2.0 / Последовательный(е) порт(ы)	0 / 3 / 1	1 / 2 / 2	1 / 2 / 2	1 / 2 / 2	1 / 2 / 2
Форм-фактор	В настольном исполнении	1RU	1RU	1RU	1RU

* - при помощи дополнительной лицензии

** - При помощи дополнительной лицензии (в базовой комплектации – 2)

*** Доступно с лицензиями Cisco ASA 5510 Security Plus

Сервисный модуль FWSM, реализующий функции межсетевое экрана, – это высокопроизводительное, интегрированное защитное решение для коммутаторов Catalyst 6500 и маршрутизаторов Cisco 7600. Этот модуль обеспечивает самую высокую в индустрии производительность – 5,5 Гбит/сек (с возможностью увеличения до 20 Гбит/сек), 1 миллион одновременно обрабатываемых соединений, 100000 соединений в секунду. Данное уникальное решение, не имеющее аналогов на рынке, ориентировано на защиту центров обработки данных банков.

Таблица 6. Основные возможности Cisco Firewall Service Module

Основные возможности	
<ul style="list-style-type: none"> • Базируется на зарекомендовавшей временем операционной системе реального времени PixOS • Поддержка до 4096 VLAN на один модуль • Создание политик для отдельных VLAN • Механизм виртуализации (до 100 виртуальных межсетевых 	<ul style="list-style-type: none"> • Отказоустойчивость и высокая доступность • Возможность ограничения использования ресурсов • Ролевое управление конфигурацией модуля • Группирование сетевых объектов и сервисов для списков контроля доступа (ACL)

экранов) <ul style="list-style-type: none"> • Тесная интеграция с модулями обнаружения атак, построения IPSec VPN и работы с SSL • Защита от подмены MAC/IP адресов (ARP Spoofing) 	<ul style="list-style-type: none"> • Масштабирование до 4-х модулей на один коммутатор • Снижение совокупной стоимости владения за счет интеграции FWSM в уже установленные в сети Catalyst 6500
---	--

Программное обеспечение Cisco IOS Firewall – это межсетевой экран с контролем состояния, интегрированный в операционную систему Cisco IOS и поддерживаемый на широком спектре моделей маршрутизаторов Cisco 800, 1600, 1700, 1800, 2500, 2600, 2800, 3600, 3700, 3800, 7100, 7200, 7400, 7500, 7600 и коммутаторах Catalyst 6500. Cisco IOS Firewall использует эффективный механизм, называемый Context Based Access Control (CBAC), позволяющий контролировать информационные потоки, проходящие через маршрутизатор, на всех уровнях, начиная с сетевого и заканчивая прикладным. На всех уровнях фильтрация осуществляется динамически, основываясь на направлении трафика, состоянии соединения и информации о предыдущих пакетах и сессиях, пропущенных маршрутизатором с Cisco IOS Firewall.

Таблица 7. Основные возможности Cisco IOS Firewall

Основные возможности	
<ul style="list-style-type: none"> • Поддержка большого числа протоколов, включая мультимедиа • Поддержка протокола IPv6 • Поддержка различных механизмов аутентификации - RADIUS, TACACS+ и т.д. • Контроль доступа по времени • Тесная интеграция с механизмами обнаружения атак, контроля качества (QoS) и построения VPN • Поддержка различных политик и списков контроля доступа для разных интерфейсов • Поддержка анализа протоколов на нестандартных портах • Трансляция сетевых адресов • Блокирование Java-апплетов • Поддержка отказоустойчивости за счет динамической смены маршрута на резервный маршрутизатор 	<ul style="list-style-type: none"> • Механизм «прозрачности» МСЭ (функционирование на канальном уровне) • Расширенная регистрация событий безопасности • Фильтрация и блокирование трафика интернет-пейджеров (IM), пиринговых приложений (P2P) и других сетевых приложений благодаря гибкому анализу на прикладном уровне • Определяемые пользователем и расширяемые политики проверки объектов протокола HTTP (длина URL, заголовки HTTP и др.) • Возможность использования конфигурации на основе CPL (Class-based Policy Language) для защиты от уязвимостей и HTTP-атак • Предотвращение DoS, атак на основе сессионных политик и политики контроля входного потока

Противодействие хакерам при взаимодействии с Интернет

Для противодействия атакам хакеров при взаимодействии автоматизированной банковской системы с сетью Интернет и соблюдении требования, указанного в п.8.2.6.6 Стандарта, компания Cisco Systems предлагает целый спектр централизованно управляемых систем обнаружения и предотвращения атак (ID&PS) – Cisco IPS 4200, Cisco ASA 5500, Cisco IDSM-2, Cisco Guard и Cisco Security Agent.

Cisco IPS 4200 является центральным компонентом решений Cisco Systems по отражению атак. На базе данного ПО построены системы обнаружения атак Cisco IDSM-2 и Cisco IDS Network Module, а также Cisco ASA 5500 (см. описание выше), который помимо всей функциональности Cisco IPS 4200 также обладают функциями межсетевого экрана, VPN-концентратора, антивируса и т.д. Наряду с традиционными механизмами в Cisco IDS/IPS используются и уникальные алгоритмы, отслеживающие аномалии в сетевом трафике и отклонения от нормального поведения сетевых приложений. Это позволяет обнаруживать как известные, так и многие неизвестные атаки. Встроенные технологии корреляции событий безопасности Cisco Threat Response, Threat Risk Rating

и Meta Event Generator помогают не только существенно снизить число ложных срабатываний, но и позволяют администраторам реагировать только на действительно критичные атаки, которые могут нанести серьезный ущерб ресурсам банковской сети.

Компания Cisco Systems – один из немногих производителей в мире, выпускающих решение по обнаружению и предотвращению атак, интегрируемое в коммутаторы локальных сетей. Модуль IDSМ-2, разработанный Cisco, устанавливается в шасси коммутатора Catalyst 6500 и обеспечивает мониторинг сетевых соединений, проходящих через него.

Таблица 8. Основные возможности Cisco Intrusion Detection Module

Основные возможности	
<ul style="list-style-type: none"> • Базируется на зарекомендовавшем временем программном коде системы Cisco IDS/IPS • Производительность – 600 Мбит/сек, 500.000 одновременно обрабатываемых соединений • Отсутствие снижения производительности коммутатора • Отражение атак канального уровня • Возможность мониторинга неограниченного контроля сетевых сегментов и VLAN • Мониторинг отказов соединения, сервиса и устройства 	<ul style="list-style-type: none"> • Защищенное обновление сигнатур атак • Разрыв соединения, а также реконфигурация межсетевого экрана, маршрутизатора или коммутатора для блокирования атаки • Тесная интеграция с модулями межсетевого экранирования и построения IPSec VPN и обработки SSL • Единое управление с сенсорами Cisco IDS/IPS, межсетевыми экранами и средствами построения VPN • Управление с помощью IDS Device Manager или CiscoWorks VPN Security Management Solution

Cisco IDS Network Module – единственное решение для обнаружения атак, предназначенное для интеграции в маршрутизаторы. Этот модуль, устанавливаемый в слот маршрутизаторов Cisco 2600XM, 2691, 2800, 3660, 3700 и 3800, обнаруживает вредоносную активность в трафике, проходящем через периметр удаленного филиала финансовой организации или небольшого банка.

Таблица 9. Основные возможности Cisco IDS Network Module

Основные возможности	
<ul style="list-style-type: none"> • Базируется на зарекомендовавшем временем программном коде системы Cisco IDS/IPS • Производительность – от 10 Мбит/сек для Cisco 2600XM до 45 Мбит/сек для Cisco 3700 • Широкий выбор настраиваемых параметров для каждой сигнатуры атак • Поддержка трафика VLAN 802.1q • Интеграция со всеми защитными функциями операционной системы IOS маршрутизатора • Автоматизированное обновление сигнатур 	<ul style="list-style-type: none"> • Мониторинг отказов соединения, сервиса и устройства • Разрыв соединения, а также реконфигурация межсетевого экрана, маршрутизатора или коммутатора для блокирования атаки • Защищенное управление с помощью SSH, SSL и IPSec • Единое управление с сенсорами Cisco IDS/IPS, межсетевыми экранами и средствами построения VPN • Управление с помощью IDS Device Manager или CiscoWorks VPN Security Management Solution

Cisco Guard позволяет отражать атаки типа «отказ в обслуживании» (DoS) в т.ч. и распределенные (DDoS), обнаруженные специализированными средствами обнаружения вторжений, в качестве которых могут выступать Cisco Anomaly Traffic Detector, Cisco IDS/IPS 42xx или Arbor Peakflow. Блокирование основано на методе «отвода» трафика и позволяет отделить вредоносные пакеты от пакетов, несущих полезные данные. Данное решение предназначено для эффективной защиты центров обработки данных и Интернет-банков.

Таблица 10. Основные возможности Cisco Guard

Основные возможности	
<ul style="list-style-type: none"> • Уникальная архитектура Multiverification Process (MVP) • Отсутствие снижения производительности защищаемой сети • Скорость обработки трафика – 1,25 миллионов пакетов в секунду (возможность масштабирования до 10 миллионов пакетов в секунду путем использования кластеров Cisco Guard) • Число параллельно обрабатываемых соединений – 1,5 миллиона • Защита от одновременной атаки со стороны свыше 100 тысяч зомби (механизм Zombie Killer) 	<ul style="list-style-type: none"> • Число динамических фильтров – 150000 (добавление 1000 фильтров в секунду) • Задержка – менее 1 мсек • Централизованное управление и интеграция с CiscoWorks SIMS • Соблюдение необходимого уровня SLA • Обеспечение услуг аутсорсинга

Защита компьютеров, обрабатывающих платежную информацию

Cisco Security Agent (CSA) – решение, предназначенное для серверов и рабочих станций, работающих под управлением ОС Windows, Solaris и Linux и участвующих в обработке платежной информации (требования, указанные в п.8.2.8). Оно объединяет различные защитные механизмы и функции в одном решении – предотвращение атак, персональный межсетевой экран, защита от вредоносного кода, контроль целостности, блокирование утечки информации через USB-порты и другие внешние устройства (PCMCIA, CD, Floppy, Zip и другие), ограничение возможностей Интернет-пейджеров (например, ICQ), обнаружение перехватчиков с клавиатуры, контроль загрузки с «чужих» носителей и т.п.

CSA позволяет отражать широкий спектр нападений – сканирование портов, переполнение буфера, троянцы и черви, DoS-атаки и других. При этом CSA построен по совершенно иному принципу, чем традиционные антивирусы и системы обнаружения атак и не использует сигнатуры для идентификации несанкционированных действий. Это в свою очередь обеспечивает защиту компьютера от неизвестных атак, сигнатуры для которых пока не написаны и отсутствуют в базах традиционных средств защиты.

Cisco Security Agent может использоваться не только для защиты серверов и рабочих станций, участвующих в обработке платежной информации, но и для обеспечения информационной безопасности банкоматов, находящихся на «чужой» территории и использующих для связи с процессинговым центром различные каналы связи (обычный или GSM-модем, выделенная линия и т.п.).

Таблица 11. Основные возможности Cisco Security Agent

Основные возможности	
<ul style="list-style-type: none"> • Интеграция с Active Directory, LDAP, NIS • Автоматическая смена политики контроля в зависимости от имени пользователя и его местоположения в сети • 2 типа корреляции событий безопасности – локальная и централизованная (от нескольких агентов) • Прозрачность установки, не требующая участия владельца компьютера • Автоматизация создания политик контроля • Управление 100 000 агентами с одной консоли управления • Инвентаризация установленного ПО • Интеграция с VPN-клиентами компаний Cisco и Check Point • Интеграция с Network Admission Control (NAC) и Cisco 	<ul style="list-style-type: none"> • Делегирование отдельных функций управления агентом пользователю • Механизм Trusted QoS • Функционирование на платформах Windows (серверы, рабочие станции, включая Tablet PC), Linux, Solaris, VMWare • Интеграция с сетевыми системами предотвращения атак • Специальная группа правил для блокирования утечки информации • Контроль загрузки с несанкционированных носителей (CD, дискета, сеть и т. д.) за счет интеграции с технологией Intel AMT



Security Monitoring, Analysis, and Response System (Cisco MARS)	
---	--

При передаче платежной информации по каналам связи п.8.2.8.7 рекомендует использовать системы криптографической защиты информации, в качестве которых может выступать решение компании Cisco, разработанное совместно с российской компанией «С-Терра СиЭсПи», и предназначенное для организации виртуальных частных сетей (VPN) на базе отечественных алгоритмов шифрования. Модуль интегрируется в маршрутизаторы Cisco ISR 2811, 2821, 2851, 3825 и 3845 и использует сертифицированное ФСБ ядро (по классам КС1 и КС2).

Таблица 12. Основные возможности Cisco Russia VPN Module

Основные возможности	
<ul style="list-style-type: none"> • Поддержка любого IOS Feature Set, начиная с IP Base • Поддержка с IOS 12.4(11)T • Поддержка IPSec ESP и AH при использовании ГОСТ 28147-89 • Полная совместимость с IKE и IPSec-решениями (RFC 2401-2412) • Поддержка NAT Transparent IPSec • Совместимость с разными системами PKI (Microsoft с CryptoPro, Notary-Pro, Валидата, RSA Keon) • Поддержка сертификатов – LDAPv3, x509v3, PKCS#7, #10 и #12, CRL • Поддержка IKE при использовании ГОСТ Р 34.10-94, ГОСТ Р 31.10-2001 • Поддержка QoS 	<ul style="list-style-type: none"> • Приоритезация мультимедийного-трафика • Отсутствие обмена данными между модулем и маршрутизатором (для критичных приложений) • Ограничение предельного уровня нагрузки на CPU для задач шифрования • Отказоустойчивость за счет автоматического переключения на резервный шлюз • Перенос IP-адресов отказавшего модуля на резервное устройство (опционально) • Поддержка протокола DPD (Dead Peer Detection) • Поддержка резервирования (между модулями в одном маршрутизаторе и между маршрутизаторами) • Интеграция с другими защитными функциями Cisco ISR – МСЭ, IPS и т. д.

Регистрация событий для проведения внутреннего аудита

В п.8.2.4.3 Стандарта указано требование регистрации попыток несанкционированного доступа. Такая регистрация необходима для проведения внутреннего аудита и расследования произошедших инцидентов информационной безопасности согласно п.10.5. Любое решение компании Cisco Systems в области информационной безопасности – системы предотвращения атак, межсетевые экраны, системы аутентификации, системы контроля содержимого и т.д., содержат в себе расширенные механизмы регистрации позволяющие фиксировать все необходимую для внутреннего аудита информацию – дату и время наступления события, адреса или имена пользователей, связанных с событием (атакуемые или атакующие), а также дополнительные детали вплоть до записи всего сетевого трафика, в котором зафиксированы следы несанкционированной активности.

Антивирусная защита

В соответствие с п.8.2.5 лучшей практикой является построение эшелонированной централизованной системы антивирусной защиты, одним из рубежей которой является антивирус, установленной не только на рабочих станциях и серверах АБС, но и в сети. Cisco Systems предлагает модуль расширения для Cisco ASA 5500, обеспечивающий защиту от вредоносных программ и контроль содержимого. Модуль CSC-SSM (Anti-X) включает в себя такие функции, как антивирус, антиспам, механизм защиты от программ-шпионов, блокирование подозрительных файлов, фильтрация и блокирование URL и др. В модуле CSC-SSM для защиты от вредоносного кода используются технологии Trend Micro – одного из лидеров рынка защиты от вредоносного ПО.

Таблица 13. Основные возможности Cisco CSC-SSM

Основные возможности	
<ul style="list-style-type: none"> • Антивирусная защита в трафике HTTP, FTP, SMTP, POP3 • Защита от программ-шпионов • Обнаружение и блокирование спама • Антифишинг, защита от перехвата и подмены идентификационной информации • Полная URL-фильтрация с использованием категорий и контролем доступа по времени • Защита в режиме реального времени web-доступа, web-почты и передачи файлов через Web 	<ul style="list-style-type: none"> • Контентная фильтрация почтовых сообщений, позволяющая избежать несанкционированной отправки конфиденциальной информации • Гибкие настройки фильтрации для реализации корпоративных политик безопасности • Централизованное управление через web-консоль • Автоматическое обновление в режиме 24 x 7

Мониторинг и расследование инцидентов информационной безопасности

Оперативное и постоянное наблюдение объектов мониторинга, требуемое согласно п.9.7.1 и п.10.9 Стандарта, осуществляется как с помощью штатных, так и специализированных средств, в качестве которых компания Cisco Systems предлагает 2 решения – Cisco Security Manager и Cisco Monitoring, Analysis and Response System (MARS).

Cisco Security Manager (CSM) – система централизованного управления всеми средствами защиты компании Cisco, пришедшая на смену CiscoWorks VMS. Отличительными особенностями CSM являются поддержка большего числа и типов устройств защиты, различные формы представления информации, механизмы обнаружения несоответствий в политике безопасности, автоматизация рутинных задач и т. д.

Таблица 14. Основные возможности Cisco Security Manager

Основные возможности	
<ul style="list-style-type: none"> • Графический интерфейс управления • Различные формы представления информации – в виде топологии сети, в виде географической карты, в виде таблицы правил • Обнаружение конфликтов в правилах политики безопасности • Обнаружение правил, не влияющих на защищенность сети • Группирование объектов • “Клонирование” настроек для ускорения внедрения средств защиты • Поддержка иерархии и наследования политик безопасности • Откат к предыдущей конфигурации • Импорт настроек из различных источников • Инвентаризация политик для уже внедренных средств защиты • Автоматическая настройка VPN-туннелей для различных топологий (Site-to-Site, Hub & Spoke, Partial Mesh, Full Mesh и т.д.) 	<ul style="list-style-type: none"> • Управление механизмами отказоустойчивости, балансировки нагрузки и контроля качества обслуживания для управляемых средств защиты Ролевое управление административным доступом с помощью Cisco Secure ACS • Автоматическое обновление средств защиты Интеграция с DCR • Интеграция с Cisco MARS для корреляции сетевых событий и заданных правил на МСЭ, что помогает более быстро принимать решения и повышает работоспособность сети • Управление и конфигурирование политик безопасности на МСЭ Cisco, включая устройства Cisco ASA 5500, Cisco PIX, модули на Cisco Catalyst 6500 • Поддержка взаимодействия с IPS Manager

Программно-аппаратный комплекс Cisco MARS предназначен для управления угрозами безопасности. В качестве источников информации о них могут выступать - сетевое оборудование (маршрутизаторы и коммутаторы), средства защиты (межсетевые экраны, антивирусы, системы обнаружения атак и сканеры безопасности), журналы регистрации ОС (Solaris, Windows NT, 2000,

2003, Linux) и приложений (СУБД, Web и т.д.), а также сетевой трафик (например, Cisco Netflow). Cisco MARS поддерживает решения различных производителей – Cisco, ISS, Check Point, Symantec, NetScreen, Extreme, Snort, McAfee, eEye, Oracle, Microsoft и т.д.

Механизм ContextCorrelation™ позволяет проанализировать и сопоставить события от разнородных средств защиты. Визуализация их на карте сети в реальном времени достигается с помощью механизма SureVector™. Данные механизмы позволяют отобразить путь распространения атаки в реальном режиме времени. Автоматическое блокирование обнаруженных атак достигается с помощью механизма AutoMitigate™, который позволяет реконфигурировать различные средства защиты и сетевое оборудование.

Таблица 15. Основные возможности Cisco MARS

Основные возможности	
<ul style="list-style-type: none"> • Обработка до 10 000 событий в секунду или свыше 300 000 событий Netflow в секунду • Сигнатурные и “поведенческие” методы обнаружения аномалий и других атак • Возможность создания собственных правил корреляции • Эскалация инцидентов (идентификация, реагирование, расследование, контроль, генерация отчетов) • Уведомление об обнаруженных проблемах по e-mail, SNMP, через syslog и на пейджер • Рольное управление через web-интерфейс • Визуализация атаки на канальном и сетевом уровнях • Поддержка Syslog, SNMP, RDEP, SDEE, NetFlow, системных и пользовательских журналов регистрации в качестве источников информации • Возможность подключения собственных средств защиты для анализа 	<ul style="list-style-type: none"> • Эффективное отсеечение ложных срабатываний и шума, а также обнаружение атак, пропущенных отдельными средствами защиты • Обнаружение аномалий с помощью протокола NetFlow • Создание и автоматическое обновление карты сети, включая импорт из CiscoWorks и других систем сетевого управления • Поддержка IOS 802.1x, NAC (фаза 2) • Распределенное отражение атак с помощью технологии Distributed Threat Mitigation • Мониторинг механизмов защиты коммутаторов (Dynamic ARP Inspection, IP Source Guard и т. д.) • Интеграция с Cisco Security Manager (CSM Policy Lookup) • Интеграция с системами управления инцидентами с помощью XML Incident Notification • Слежение за состоянием контролируемых устройств • Интеграция с Cisco Incident Control System (ICS)

Прогнозируемость развития проблем и оценка их влияния на бизнес-цели

Для прогнозирования развития проблем с информационной безопасностью и оценки их влияния на бизнес финансовых учреждений банковской системы РФ компания Cisco Systems предлагает специализированное решение CiscoWorks Security Information Management Solution (SIMS), которое представляет собой масштабируемую и централизованно управляемую систему сбора, анализа и корреляции событий безопасности, получаемых от средств защиты различных производителей (Cisco, Check Point, ISS, NetScreen, Symantec и т.п.). В качестве источников данных для SIMS могут выступать межсетевые экраны и маршрутизаторы, сетевые и хостовые системы обнаружения атак, системы построения VPN и Web-сервера, журналы регистрации событий операционных систем Windows и Unix. Также существует возможность подключения к SIMS своих собственных средств защиты информации, в т.ч. и российского производства.

Таблица 16. Основные возможности CiscoWorks SIMS

Основные возможности	
<ul style="list-style-type: none"> • Агрегирование 20.000 типов сигналов тревоги в 9 категорий 	<ul style="list-style-type: none"> • Более 250 встроенных шаблонов отчетов

<ul style="list-style-type: none"> • Объединения связанных событий в одно метасобытие • Устранение избыточной информации • Различные виды анализа и сопоставления данных от разнородных средств защиты • Анализ с точки зрения ценности для бизнеса • Встроенные и создаваемые пользователем правила корреляции событий • Расширенные механизмы уведомления 	<ul style="list-style-type: none"> • Возможность поставки в виде программно-аппаратного комплекса • Проверка соответствия различным стандартам (например, SOX, GLBA, HIPAA, FISMA и т. п.) • Поддержка технологии Network Admission Control (NAC) • Интеграция с HP OpenView • N-уровневая архитектура с контролем состояния удаленных компонентов • Интеграция с системами управления инцидентами (например, Remedy HelpDesk)
---	--

Контролируемость защитных средств

Для контроля средств обеспечения информационной безопасности, используемых для защиты автоматизированной банковской системы, компания Cisco Systems предлагает специализированное решение Cisco Configuration Assurance Solution, позволяющее повысить защищенность и работоспособность сети на основе проверки соответствия текущих настроек сетевого оборудования и требований существующих политик или международных стандартов безопасности. Cisco CAS диагностирует ошибки в настройке оборудования, неэффективности в работе, проблемные места в защите, помогая оценить защищенность сети на соответствие требованиям HIPAA, ISO 17799, ITIL/BS15000 и др.

Таблица 17. Основные возможности Cisco Configuration Assurance Solution

Основные возможности	
<ul style="list-style-type: none"> • Обнаружение ошибок в настройке сетевого оборудования и средств защиты • Проверка корректности используемых сетевых политик безопасности (например, на Cisco Pix, Cisco ISR или Cisco Catalyst) • Аудит решений третьих фирм (Check Point, Juniper, Nokia, Nortel и т. д.) • Создание отчетов по соответствию нормативным документам, таким как Sarbanes-Oxley, HIPAA, FISMA и др. • Поддержка более 400 правил для стандартных протоколов и технологий (IP, RIP, OSPF, IGRP, EIGRP, BGP, ACL, HSRP, SNMP, AAA, RADIUS, Kerberos, TACACS+, VLAN, VPN, QoS и др.) 	<ul style="list-style-type: none"> • Доступ к сетевому оборудованию через SSH или SNMP • Поддержка ключевых процессов архитектуры управления ИТ, включая ITIL/BS15000 и ISO 17799 • Импорт данных для последующего анализа и аудита от Cisco NetFlow FlowCollector, CiscoWorks RME, Campus Manager, Cisco Network Connectivity Center, Cisco Info Center • Рассылка уведомлений в случае критических ошибок на e-mail или пейджер • Возможность персонализированной настройки правил проверки, частоты и времени проведения аудита, создаваемых отчетов • Создание собственных политик безопасности для последующих проверок

Вторым решением является CiscoWorks Network Compliance Manager (NCM) – web-приложение из семейства продуктов CiscoWorks, позволяющее отслеживать конфигурацию и изменения ПО в многовендорной сетевой инфраструктуре на соответствие требованиям различных государственных, международных и корпоративных стандартов не только в области безопасности, но и в области ИТ. Помимо проверки NCM позволяет также сформулировать рекомендации по их корректировке. Внедрение NCM помогает идентифицировать изменения в настройке сетевого оборудования, лучше понимать тенденции в сетевой инфраструктуре, что позволяет оперативно устранять бреши в защите сети и повышает стабильность ее работы.

Таблица 18. Основные возможности Cisco Network Compliance Manager

Основные возможности	
<ul style="list-style-type: none"> • Автоматическое обнаружение сетевых устройств (auto-discovery) • Построение карты сети для упрощения поиска и устранения неисправностей • Импорт информации о сети из CiscoWorks DCR • Простота в отслеживании изменений в конфигурации устройств • Генерация различных отчетов, включая необходимые для проверки соответствия нормативным требованиям (SoX, VISA CISP/PCI, HIPAA, GLBA, FISMA, ITIL, CobiT, COSO и др.) • Интеграция с приложениями CiscoWorks (CiscoWorks LMS, Device Center, CiscoView) • Поддержка ролевого управления 	<ul style="list-style-type: none"> • Централизованное управление ACL • Высокая масштабируемость (контроль сетей из десятков тысяч узлов) • Обеспечение отказоустойчивости • Аудит различных типов оборудования – межсетевые экраны, маршрутизаторы, коммутаторы, VPN, точки беспроводного доступа и т. п. • Анализ оборудования 35 различных производителей – Cisco, 3Com, Check Point, Crossbeam, Enterasys, Extreme, HP, Juniper, Nortel, ZyXEL и т. д. • Идентификация критических рисков и возможных уязвимостей с последующей расстановкой приоритетов

Своевременность обнаружения проблем

С целью своевременного обнаружения проблем, потенциально способных повлиять на ее бизнес-цели, компания Cisco предлагает специальный сервис IntelliShield Alert Manager, позволяющий освободить технических специалистов от постоянного поиска и отслеживания уязвимостей в продуктах, используемых в корпоративной сети компании. Основное отличие Cisco Security IntelliShield Alert Manager Service от множества других сервисов – уведомление только о тех уязвимостях, которые присущи именно Вашему программному обеспечению. IntelliShield Alert Manager состоит из 4-х компонентов – защищенного web-портала, скрытой от пользователя инфраструктуры сбора и анализа информации об угрозах, базы данных уязвимостей и системы документооборота, обеспечивающей отслеживание, связывание, уведомление об уязвимости и контроль методов устранения.

Таблица 19. Основные возможности Cisco IntelliShield Alert Manager Service

Основные возможности	
<ul style="list-style-type: none"> • Постоянно пополняемая всесторонняя база данных уязвимостей – информация о 16 000 уязвимостях с мая 2000 г. • Информация предоставляется по 18 500 версий 5500 продуктов 1700 известных разработчиков • Совместимость с CVE • Автоматическая генерация отчетов • Включение в уведомления и отчеты ссылок на обновления • Возможность интеграции уведомлений от IntelliShield Alert Manager в собственные приложения при помощи XML 	<ul style="list-style-type: none"> • Настраиваемые интеллектуальные фильтры (Smart Filters) – поиск и выборка по любым параметрам (производитель, продукт, версия, ключевые слова, критичность, дата и т. д.) • Встроенная система ранжирования рисков • Различные варианты рассылки уведомлений об уязвимостях (e-mail, пейджер, SMS) • Различные пороговые значения для генерации уведомлений с целью минимизации получаемой информации

Обучение персонала

Для эффективной реализации п.8.2.2.11 Стандарта компания Cisco Systems предлагает авторизованное обучение по целому ряду программ и курсов в области информационной безопасности. Такое обучение можно пройти в авторизованных учебных центрах компании Cisco Systems, а также в сетевых академиях Cisco Systems (Cisco Networking Academy), расположенных на территории России. Курсы позволяют подготовиться к сдаче экзаменов на получение различных уровней сертификации по

безопасности Cisco Specialist или Cisco Certified Security Professional (CCSP). Статус Cisco Specialist может быть получен по одному из следующих направлений:

- Cisco Advances Security Field Specialist;
- Cisco Security Sales Specialist;
- Cisco Firewall Specialist;
- Cisco Security Solutions and Design Specialist;
- Cisco IPS Specialist;
- Cisco VPN Specialist.

Существует также ряд дополнительных курсов, рекомендованных инженерам, готовящимся к сдаче экзамена на высший статус эксперта Cisco Certified Internetwork Expert (CCIE) Security. Завершение обучения по программам CCNA и Cisco Specialist позволяет получить статус INFOSEC Professional (стандарт образования 4011), поддерживаемый Агентством национальной безопасности США (NSA) и Комитетом США по национальным системам безопасности (CNSS).

ЗАКЛЮЧЕНИЕ

Сегодня инфокоммуникации стали центром развития новых технологий, в корне меняющих методы взаимодействия и ведения бизнеса в среде финансовых организаций. Уверенность в том, что бизнес-процессы и ресурсы банка защищены от посягательств внешних и внутренних злоумышленников и воздействия вредоносных программ является критическим фактором в современном мире. Этот постулат подтверждает и стандарт «Обеспечение информационной безопасности организаций банковской системы Российской Федерации», принятый Банком России и нацеленный на повышение уровня защищенности российских банков и защиту банковской тайны вкладчиков.

Компания Cisco Systems, в отличие от ряда других поставщиков, предлагает своим заказчикам не точечные продукты для защиты отдельных участков автоматизированной банковской системы и ее пользователей, а комплексное решение, интегрируемое в инфраструктуру финансовой организации для обеспечения информационной безопасности бизнеса на всех уровнях.

Self-Defending Network (SDN) – стратегия компании Cisco Systems, нацеленная на защиту бизнес-процессов в условиях растущей угрозы со стороны вредоносных программ и злоумышленников, воздействующих на бизнес-процессы банка изнутри и извне. Учитывая скорость распространения современных угроз, например червей и вирусов, средства защиты компании Cisco Systems строятся на основе проактивного подхода, заключающегося в предвосхищении угроз, а не в борьбе с их последствиями. В основе SDN лежит интеграция механизмов безопасности в сетевую инфраструктуру, в которой все ее элементы – от персонального компьютера до сетевого оборудования, участвуют в процессе обеспечения защищенности, устойчивости и непрерывности бизнеса. Стратегия Self-Defending Network заключается в автоматизации процесса обеспечения информационной безопасности за счет обнаружения угроз, реагирования соответственно уровню критичности, изолирования зараженных или взломанных узлов, и реконфигурации сетевых устройств с целью предотвращения повторных атак.

ДОПОЛНИТЕЛЬНЫЕ ИСТОЧНИКИ ИНФОРМАЦИИ

Решения Cisco Systems по информационной безопасности

<http://www.cisco.com/go/security>



Cisco Systems
Россия, 113054 Москва
бизнес центр "Риверсайд Тауэрз"
Космодамианская наб., 52
Стр. 1, 4-й этаж
Тел.: +7 (095) 961 14 10
Факс: +7 (095) 961 14 69
Internet: www.cisco.ru
www.cisco.com

Cisco Systems
Казахстан, 480099 Алматы
бизнес центр "Самал 2"
Ул. О. Жолдасбекова, 97
блок А2, этаж 14
Тел.: +7 (3272) 58 46 58
Факс: +7 (3272) 58 46 60
Internet: www.cisco.ru
www.cisco.com

Cisco Systems
Украина, 252004 Киев
бизнес центр "Горайзон Тауэрз"
Ул. Шовковична, 42-44, этаж 9
Тел.: (044) 490 36 00
Факс: (044) 490 56 66
Internet: www.cisco.ua
www.cisco.com

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on
Cisco Connection Online Web site at <http://www.cisco.com/>
<http://www.cisco.ru/>

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2004 Cisco Systems Inc. All rights reserved. Printed in Russia. Cisco IOS is the trademark; and Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners.